Operational Risk Management

Rolf van den Heever & Janina Slawski

Or comprehensive yet pragmatic by another name
Agenda slides look like this

1. Objectives of this talk
2. Banking context
3. Insurance context
4. Overall conclusions
Objectives of this talk

• We consider some of the operational risk management regulatory requirements introduced for banks and insurance companies.

• We discuss how these requirements have been managed by banks and explain how the operational risk management is also used to quantify operational risk capital.

• We explore the operational risk management requirements of solvency II for insurance companies.

• We conclude that operational risk and capital management requires a pragmatic control framework that relies on solid governance and control.
Banking context
Banking context

1. Introduction and objective
2. Governance and operational risk control process
3. Risk classification and control methodologies
4. Scenario analyses
5. Operational risk impact estimation
6. Aggregation
7. Validation
Introduction and objectives

Why do banks need operational risk management?

- Banks business strategies (and implied risk strategy) necessitate risk management.
- Spectacular operational failures highlight these implied risks.
- Regulators and other stakeholders respond with significant requirements.
- Banks are required to comply to laws and regulations.
- Good operational risk management reduces frictions and increases shareholder return.

To develop and maintain an operational risk management framework:

- Consider the business and regulatory objectives
- Obtain details of approaches and assumptions
- Develop synthesis
- Test hypothesis (this includes review and validation) to objectives
- Repeat

Detailed regulatory requirements: http://www.bis.org/publ/bcbs128b.pdf par 644 to 683
Governance and Risk Control

Common industry practice for sound operational risk governance often relies on three lines of defence

(i) business line management,

(ii) an independent corporate operational risk management function and

(iii) an independent review.

Depending on the <firm’s> nature, size and complexity, and the risk profile of a bank’s activities, the degree of formality of how these three lines of defence are implemented will vary.

The Basel committee promotes the three lines of defence governance framework

• Each firm needs to carefully consider implementation as one size definitely does not fit all. (Pragmatism!)

• The independent corporate operational risk management function will rely on legal, compliance, internal audit and other functions.

• Clear responsibilities must be outlined to avoid duplication of effort and cost.
Banks strive to articulate operational risk appetite consistently with other risk appetite statements but exceptions will remain

- The quantification of operational risk proves problematic given the low frequency high severity nature of the risk, yet return periods are considered. (Pragmatism!)
- Even though an operational risk management framework can address reputational risk, operational risk capital is not a proper mitigant or risk appetite benchmark.

**Principles of Risk Control**

**The Board of directors**

1. Take the lead in establishing a strong operational risk management culture.
2. The ORMF must be fully integrated into the firm’s overall risk management processes.
3. Establish, approve and periodically review the Framework to ensure it is implemented effectively.
4. Approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types, and levels of operational risk that the bank is willing to assume.

Ref: [http://www.bis.org/publ/bcbs195.pdf](http://www.bis.org/publ/bcbs195.pdf) par 20
Principles of Risk Control

Senior Management

5: Develop governance for consistently implementing and maintaining operational risk. This includes the creation and maintenance of a second line of defence.

6: Ensure the identification and assessment of the operational risk is inherent in all material products, activities, processes and systems throughout the life cycle of each.

7: Ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk.

8: Implement a process to regularly monitor OR profiles and material exposures to losses.

9: Implement a strong control environment that utilises policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.

10: Maintain business resiliency and continuity plans.

11: Public disclosures should allow stakeholders to assess the firm’s approach to operational risk management.

REF: HTTP://WWW.BIS.ORG/PUBL/BCBSI95.PDF PAR 20
### Basel II definition
Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk.

<table>
<thead>
<tr>
<th>Event-Type Category (Level 1)</th>
<th>Categories (Level 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Fraud</td>
<td>Unauthorised Activity</td>
</tr>
<tr>
<td></td>
<td>Theft and Fraud</td>
</tr>
<tr>
<td>External Fraud</td>
<td>Theft and Fraud</td>
</tr>
<tr>
<td></td>
<td>Systems Security</td>
</tr>
<tr>
<td>Employment Practices and Workplace Safety</td>
<td>Employee Relations</td>
</tr>
<tr>
<td></td>
<td>Safe Environment</td>
</tr>
<tr>
<td></td>
<td>Diversity &amp; Discrimination</td>
</tr>
<tr>
<td>Clients, Products &amp; Business Practices</td>
<td>Suitability, Disclosure &amp; Fiduciary</td>
</tr>
<tr>
<td></td>
<td>Improper Business or Market Practices</td>
</tr>
<tr>
<td></td>
<td>Product Flaws</td>
</tr>
<tr>
<td></td>
<td>Selection, Sponsorship &amp; Exposure</td>
</tr>
<tr>
<td></td>
<td>Advisory Activities</td>
</tr>
<tr>
<td>Damage to Physical Assets</td>
<td>Disasters and other events</td>
</tr>
<tr>
<td>Business disruption and system failures</td>
<td>Systems</td>
</tr>
<tr>
<td>Execution, Delivery &amp; Process Management</td>
<td>Transaction Capture, Execution &amp; Maintenance</td>
</tr>
<tr>
<td></td>
<td>Monitoring and Reporting</td>
</tr>
<tr>
<td></td>
<td>Customer Intake and Documentation</td>
</tr>
<tr>
<td></td>
<td>Customer / Client Account Management</td>
</tr>
<tr>
<td></td>
<td>Trade Counterparties</td>
</tr>
<tr>
<td></td>
<td>Vendors &amp; Suppliers</td>
</tr>
</tbody>
</table>

Adopted from the Basel II definitions
Observations

• Many operational risks are already considered implicitly as part of other risk event types. These boundary conditions must be clearly articulated. Banks often double count risks.

• Operational risk arises from people, process, systems failure and external events. Classification of an operational risk event can therefore be problematic. The predominant root cause is generally used to classify operational risk. Consistency is key.

• The number of risk categories used vary greatly between organisations. This makes cross comparisons between organisations difficult. In particular banks generally consider tax risk separately and include legal, compliance and regulatory risk as part of operational risk.

• Reputational risk is generally included in the operational risk framework but operational risk capital is not a proper mitigant or risk appetite measure.

• A detailed taxonomy is required to obtain approximately consistent interpretations of risk event types and to ensure complete risk universe assessments.

• Operational risks in shared services are often double counted which can result in a duplication of risk management and capital yet enhances control.

• Loss events resulting from failure to treat customers fairly is often the biggest risk for retail organisations (precipice bonds / payment protection insurance) and internal fraud on a trading desk (running unauthorised open positions) for investment banking operations.

Ref: HTTP://WWW.BIS.ORG/PUBL/BCBS196.PDF
Risk control methodologies

Observations

- Risk control is the key element of OR management framework. These include internal audit reports, risk identification and self assessment, scenario analyses and key business and control indicators.

- An operational risk framework that does not emphasize risk control is fundamentally flawed (such as simply setting OR capital based on turnover).

- Risk control is both business unit and shared service specific.

- Different controls are required for the management of typical losses compared to unexpected losses. Typical losses can be budgeted for but for unexpected losses the old maxim of prevention is better than cure is key. Scenario analyses are key in this regard.

- Significant flexibility and ease of use is required in the proposed operational risk management IT solutions. Firms often roll out web based assessment tools that are too cumbersome, slow and not scalable.

- It is difficult to maintain a constant energy for control improvements as most significant wins are made in the initial phases of the project.

- It is difficult to assess the return on investment due to the infrequent occurrence of severe operational risks. Strong regulatory oversight is therefore required for this grudge purchase.

- The frequency of operational risk assessment varies but as a minimum are annual.
OR quantification methodologies

Natural disasters are never the same nor is historic experience a guide to future disasters yet actuaries are prepared to price catastrophe insurance. Comprehensive yet pragmatic!

**Loss Distribution Approach (LDA)**

**Internal data**
- Loss Database
- General Ledger

**Business environment and control factors**
- Analysis of relationship with loss data
- Distribution adjustment or scorecard

**External data**
- Clean Projected Data

**Scenario analysis**
- Clean Projected Data and control self assessment

**Loss Distribution Approach**

For each business area and material risk event type:

\[ S_1 = \sum_{i=0}^{N} X_i + \sum_{i=0}^{M} Y_i \]

Each marginal distribution \( S \) is adjusted for dependency to other marginal distributions through distribution function rank ordering (copula).

\[ S = \sum_{BU} \sum_{RET} S_{BU.RET} \]

\[ S_2 = \sum_{i=0}^{N} X_i \]

**Credibility:**

Ref: R van den Heever; ASSA Sessional Discussion 16 April 2007
Loss Models by Klugman, Panjer & Willmot
Some observations on the use of internal data

- The key objective is to estimate future operational risk experience. Historic loss data may provide some insight. Comprehensive data are required yet interpretation must be pragmatic.

- Many banks have already implemented these approaches and obtained approval from 2008 onwards.

- Internal loss data are available for management information in the control framework. These data are used in both the loss distribution and scenario approaches. A strong second line of defence is required to assimilate the loss data.

- The internal loss data are analysed using statistical techniques to produce loss distributions that present future anticipated loss experience. Different distributions are used to represent loss experience. For example frequency of loss, severity of typical loss and severity of extreme loss.

- Internal data may be enhanced with external data to provide a wider indication of potential losses.

- Insurance has been found to have a marginal impact in the reduction of operational internal loss experience and therefore has only a marginal impact on capital assessments. Many organisations ignore the benefits of insurance.
Use of external data

- Key objective: improve the estimation through benchmarking based on relevant external data

- A number of data sources exists:
  - BBA (some support from British Banks);
  - ORX (independent initiative with high admission criteria)
  - OpVaR (some US bias)
  - ABI (recent addition for insurance companies), etc.

- External data provides an indication of potential experience. Key challenge is to assess equivalent impact in organisation. Some organisations evaluate each and every on a case by case basis to develop relevant loss data.

- Extreme losses can be used to set an upper limit for losses using EVT but very conservative (some very well regarded banks do use EVT)

- The specific details of large loss events will provide an indication of the types of scenarios and control breakdowns that can lead to severe events to support the scenario analysis process.
Use of business environment and control factors

- Key objective: Estimate future expected experience by incorporating key indicators.

- The effectiveness of internal controls are evaluated as part of the control self assessment process. In addition, relevant business environment factors are evaluated through representative indicators.

- The relationship between indicators and loss experience is analysed statistically to identify explanatory relationships i.e. what is the impact on incurred losses of a change in the indicators. This requires the collection of historical data based on the business processes and takes some time to achieve.

- These relationships are interrogated and established by the operational risk team (2nd line) and verified by 3rd line.

- These relationships will be used to:
  - adjust the output from the modelling of internal loss data to ensure that it is forward looking rather than based on the historical risk profile; and
  - adjust the capital estimate for significant changes in the risk profile in the intervening periods between scenario analyses.
## Scenario Analyses (by business and risk)

<table>
<thead>
<tr>
<th>Consider sources of information:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Market data</td>
</tr>
<tr>
<td>Internal historic event data</td>
</tr>
<tr>
<td>External historic event data for other financial institutions. “If it happened there can it happen here?”</td>
</tr>
<tr>
<td>Key control weaknesses</td>
</tr>
<tr>
<td>Strategy</td>
</tr>
<tr>
<td>Business plans</td>
</tr>
<tr>
<td>Business trends i.e. legal, technological, political, demographic etc.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Establish how the risk will manifest in terms of:</th>
</tr>
</thead>
<tbody>
<tr>
<td>classification</td>
</tr>
<tr>
<td>origination</td>
</tr>
<tr>
<td>duration</td>
</tr>
<tr>
<td>frequency and impact</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scenario preparation:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify key weaknesses that can lead to risk events.</td>
</tr>
<tr>
<td>Obtain supporting evidence from sources of information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scenario generation</th>
</tr>
</thead>
<tbody>
<tr>
<td>List all key weaknesses</td>
</tr>
<tr>
<td>Vote on most relevant weaknesses</td>
</tr>
<tr>
<td>Develop scenario based on these weaknesses.</td>
</tr>
<tr>
<td>Consider outcome in terms of career duration and worst case.</td>
</tr>
<tr>
<td>Identify all areas of impact on the balance sheet and profit and loss and their duration.</td>
</tr>
</tbody>
</table>

### Scenario Impact:
- Consider potential management actions
- Establish the gross and net financial assessment

---

**2011 CONVENTION**

**8 – 9 NOVEMBER**
Use of scenario analyses

- Key objective: Estimate future expected experience.
- The operational risk team provides key oversight of this process and care is required not to guide business to a predetermined outcome.
- Business areas consider scenarios relevant to their risk exposure. Internal and external loss details are presented. Results are challenged based on control indicators. For example, poor audit reports will increase the loss assessment.
- Scenario analyses are used extensively in the quantification of operational risk. Different statistics (mode and percentiles) are obtained through the exercise and loss distributions are estimated based on the output.
- The maximum of the loss distribution is also estimated (but unlimited loss distributions are very common).
- Many large European banks use this approach.
- Scenario analyses are also used to estimate the expected correlation in stress circumstances through the application of a series of group wide stressed scenarios. (This method is more prevalent in banks than in insurance companies).
- The output of scenario analyses are also used to improve the risk control framework. (This is only possible with proper governance structures).
Use of correlation and aggregation

- Key objective: Combine marginal distributions and allow for known dependencies.
- One approach is through setting a function between the rank of one distribution and that of
  another i.e. C(F(X);F(Y)) of the cumulative distribution functions (often referred to as a
  copula).
- Another approach is through a causal framework.
- The ranked correlation coefficient is estimated using scenario analyses as empirical data
  are currently too sparse.
- As a consequence the collective risk model can be derived by individual risk event type, by
  business area and subsequently by division and then group. A distribution with all statistics
  is available for each of these combinations. This approach is already embedded by many
  of the large European banks.
- Value at Risk, shareholder deficit, expected loss and other metrics can be derived and
  tolerance levels set for each of these.
- Many banks applying for Advanced Measurement Approach (internal model) already have
  these frameworks in place.
Observations based on working with other organisations

- Key objective: Obtain independent assurance that the quantification is fit for purpose.
- Validation at group level can be very thorough. The operational risk team has verified the business input. Internal audit verifies the process. Due to limited internal resource many organisations use professional advisors as well.
- Comprehensive supporting evidence is required to provide a compelling argument for operational risk quantification. Many of the arguments lack supporting evidence and are often attributed solely to “expert judgement”.
- Stress testing forms a key part of the validation of the operational risk framework. In addition actual issue remediation also provides validation of the framework quality.
- Embedding the framework in the organisation is key (the use test).
- Validation frameworks include validation of:
  - data inputs with particular focus on key risk indicators,
  - model design and testing,
  - stress testing
  - actual issue resolution and
  - analysis of change.
Conclusions

- OR frameworks have been part and parcel of bank management for many years.
- Banks have invested in processes to quantify operational risk capital as well and these processes are now embedded in many of the larger organisations.
- The emphasis on control and proper governance is now more important than ever as operational risk event remain.
- OR quantification is driven by exposures to extreme events and any quantification is therefore subject to high levels of uncertainty.
- Appropriate scenario analyses and stress tests are required to ensure that risk assessments capture potential severe tail events.
- The boundary between operational risk capital and reserve margins or provisions must be clearly articulated.
- The correlation assumptions built into the model are pragmatic.
- Typical losses should be incorporated into budgeting and product pricing.
- The framework should incentivise the mitigation of operational risk exposure. This is generally achieved by linking key risk indicator and audit results to objectives.
Insurance context
Agenda: Insurance Context

1 Management of Operational Risk
2 Operational Risk Capital Requirements
3 Conclusions
Insurance context: Management of Operational Risk
Solvency II / SAM Context

• Insurers are required to have in place an effective system of governance that provides for sound and prudent management of the business. The “system of governance” should cover:
  • Organisational structure:
    • segregation of responsibilities, transmission of information, continuity and contingency plans, fit and proper requirements
  • Risk management
  • Own risk and solvency assessment
  • Internal control
  • Internal audit
  • Actuarial function
  • Outsourcing
### Application to Operational Risk

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisational structure</td>
<td>Existing structure should be assessed for appropriateness and be subject to ongoing review</td>
</tr>
<tr>
<td>Own risk and solvency assessment</td>
<td>Assessment of operational risk together with other risks</td>
</tr>
<tr>
<td>Internal control</td>
<td>Are policies and procedures in place and being followed for all risk categories – not just operational risk</td>
</tr>
<tr>
<td>Internal audit</td>
<td>Evaluation of adequacy of the control system</td>
</tr>
<tr>
<td>Actuarial function</td>
<td>Quantification and reporting on exposures; modelling of risk</td>
</tr>
<tr>
<td>Outsourcing</td>
<td>Management of operational risk related to outsourced functions</td>
</tr>
</tbody>
</table>
Risk Management System

• Insurers should have in place an effective risk management system comprising strategies, processes and reporting procedures necessary to identify, measure, monitor, manage and report, on a continuous basis the risks, at an individual and at an aggregated level, to which they are or could be exposed, and their interdependencies

• The risk management system should be effective and well integrated into the organisational structure and in the decision-making processes of the insurer.

• The risk-management system should cover at least the following areas:
  (a) underwriting and reserving;
  (b) asset–liability management;
  (c) investment, in particular derivatives and similar commitments;
  (d) liquidity and concentration risk management;
  (e) operational risk management;
  (f) reinsurance and other risk-mitigation techniques.

• The written policy on risk management should comprise policies related to all the above areas
Risk Management Framework

Reference: Amlin Annual Report, 2009
Risk Framework

- **Risk Policy and Strategy**
  - Written policy
  - Balance between business imperatives versus tight risk controls
  - Risk responsibilities e.g. management from the centre versus management within business units
  - Risk governance

- **Risk Appetite and Tolerance**
  - Quantification of potential risks in terms of magnitude and likelihood
  - Degree to which controls mitigate risk
  - Management decision making on acceptance of risk
Operational Risk Categories

- Financial reporting
- Taxation
- Internal fraud
- External fraud
- Premises
- Data and records
- Transactions
- Product development
- Payments
- Third party suppliers
- Technology
- People
- Legal
- Regulatory
- Compliance

Operational risk should include legal risks, and exclude risks arising from strategic decisions, as well as reputation risks.
Risk Assessment Process

• **Identify** the risks to which the insurer is exposed
• **Assess** the impact and the likelihood of the risk
  • For example, score each out of 5 and multiply
  • What controls are in place and how effective are they?
  • Management self assessment of adequacy of controls
• **Response:** rank the risks and agree which risks require action to be taken and which risks management is willing to accept
• **Report** regularly on the risk environment
  • Quarterly Risk Committee meetings
  • Risk dashboards reflecting status of risks and controls
  • Updates on actions being taken
  • Report on actual events and near misses
    • Analyse what went wrong, what should have happened to prevent the occurrence, what changes are required to the risk environment?
• **Review:** take stock of risk approaches on an annual basis
  • Audit of risk management processes
Governance

- Committees, reporting structures, oversight required
- Accountability and ownership:
  - Assignment of risk ownership within business
  - Owners of both risks and controls
  - Management self assessment of risks and controls
- Communication:
  - Risk dashboards
  - Incidents
  - Updates on governance
- Infrastructure: risk systems
  - Formalise risk ownership and assessments
  - Monitoring of risk exposures
  - Dashboard overviews
- Challenge: key to making risk management work in practice
Ownership and Challenge

• There must be a robust review of the risk environments
• Commonly held views and historical ways of doing things must be challenged
• The risk approach should provide a supportive environment for issues raised
  • Identification of issues and appropriate actions is key
  • Over-reaction can drive risks “underground”
• Risk management must be practical and “useful”
• A “tick box”, compliance focus will drain energy away from the real issues
• Thinking creatively about risk management may highlight business opportunities
Insurance context: Operational Risk Capital Requirements
Operational Risk Capital Requirements

- In the QIS5 and SAQIS1 standard formula, operational risk capital requirements are added to the Basic Solvency Capital Requirement.
- The capital requirement for operational risk is calculated as:
  - Minimum of:
    - 30% of Basic Solvency Capital Requirement, and
    - “Op” (basic operational risk charge for all business other than life insurance where the investment risk is borne by the policyholders)
  - Plus:
    - 25% of the amount of annual expenses incurred during the previous 12 months in respect life insurance where the investment risk is borne by the policyholders.
  - “Op” calculation is based on volume measures being a maximum of two calculations using:
    - earned premiums, and
    - technical provisions excluding the risk margin.
Conclusions from QIS 4

• The average per country of the percentage of the operational risk capital charge to the total SCR ranged from 5% to 10%

• One Member State responded that the operational risk charge as currently calibrated in the standard formula understates the operational risk requirement as set by the undertakings’ own internal model sometimes by more than half

• In relation to the formula, respondents stated that:
  • The standard formula is too simplistic, since it is not risk sensitive, and rewards low pricing and reserving
  • The consideration of 100% correlation with other risks is not appropriate
  • The formula does not take into account the quality of the operational risk management processes of each undertaking, nor does it encourage the development of good risk management practices
  • The maximum of 30% of the BSCR for the capital charge is considered too high
  • The formula does not reflect the wide spectrum of operational risks that can materialise within an undertaking

• Conclusion:
  • The standard formula for operational risk is a blunt tool that will over / under-state risk for individual entities
South African Context

• Results of and comments on SAQIS1 still to be released
• Standard formula versus internal model?
  • Hard data can be used for internal model development for other risks, but less hard data is available on operational risk
  • Standard curve fitting and projection methodologies not as applicable to operational risk
  • Inclusion of more “soft” data and qualitative assessments is required
  • Insurers are probably more likely to follow the standard formula for operational risk even if an internal model is used for other risks
Example of Operational Risk Quantification

- Application of the banking AMA model in the insurance context
- **Key Risk Scenarios** (KRSs) are the main driver of the model
  - Individual business areas develop KRSs
  - KRSs have expected and unexpected (1 in 7, 1 in 20, 1 in 100) values
  - Curves are fitted to frequency and severity and then combined
    - Frequency: Poisson distribution
    - Severity: Pareto distribution
  - The Panjer algorithm is used to combine the overall loss distributions
  - Common shocks are used for correlation assumptions
Operational Risk Quantification

- Management Self Assessments
- Key Indicators
- External Risk Events
- Internal Risk Events

Key Risk Scenarios

Capital Model

Capital required
Operational Risk Quantification

• Key Risk Scenarios:
  • “Brain storming” exercise
  • Business risk owners consider what could happen and the level of sufficiency of a scenario

• Consistency with stress tests for other risk categories:
  • For example, underwriting capital is held for earthquake and pandemic risks
  • What would be the operational consequences of these events e.g. appointing temporary staff to handle claims?
  • Are the combined underwriting and operational risk capital amounts sufficient for these events?

• Actuarial team can assist:
  • in quantifying the financial impact of scenarios
  • fitting and combining curves
  • adding correlation and impact of stress events
  • allocation of capital to business units
Key Risk Scenarios: Examples

- Third party supplier risk
  - Electrical fire after a contractor has replaced a geyser results in a house burning down
  - Outsourced administration fails to pick up unmatched position on investment linked policies

- Transactions risk:
  - Underwriter fails to follow process and underwrites a property without special acceptance being requested for cover above the reinsurance treaty limit

- External fraud:
  - Client burns down a house in order to collect insurance proceeds

- Regulatory risk:
  - Co-insurance arrangements are deemed as collusion and subject to a Competitions Act fine
Capital Allocation

• Basis for allocation
  • Business volume: premium, fees, etc.
  • KRSs per business unit
  • Key indicators
  • Management self assessments and actions required
  • Actual and near-miss events

• Benefits of allocation process:
  • Increases understanding of relative business risks
  • Higher risk businesses should deliver a higher return to justify take on of risk
  • Focuses attention on qualitative data influencing allocation

• Issue: penal capital allocation can drive the underplaying of potential risks
Benefits of Quantification

• Assists in **understanding and improving the controls** in place:
  • Scenarios are often based on what has happened in the past – helps to confirm that current controls would prevent re-occurrence
  • Get business risk owners thinking about the risks in their business
  • Brainstorming approach encourages the “outside the box” thinking
  • What could actually go wrong despite current controls?
  • How would events be picked up and how would controls operate in practice?
  • What else can be put in place to prevent the occurrence?
• Is the **standard formula** giving capital figures appropriate to the actual risk faced by the business?
• Assessment of **planned improvements** to risk environment
  • Benefit of risk enhancement e.g. less capital required, less management time, etc. versus cost of implementation
Insurance context: Conclusions
Conclusions

• Insurance legislation is less prescriptive than Basel, generally and in respect of operational risk
• Operational risk should be managed within an overall sound risk management framework
• Risk management should be practical – an approach with too much of a compliance focus may prevent real issues from being identified
• There is less hard data for operational risk so more creativity and use of qualitative data is required
• The more that management owns and thinks about operational risk, the more robust the risk environment will become
Overall Conclusions
Overall Conclusions

• Operational risk management frameworks similar between insurance and banking legislative requirements
  • Use the specifics of Basel where this in not equivalent detail in Solvency II guidance
• Focus on risk management rather than quantification for calculation of capital requirements
• Risk controls are key to risk mitigation
  • By the time you need operational risk capital, it’s too late...